UNITED STATES DEPARTMENT OF COMMERCE
Patent and Trademark Office
Address: COMMISSIONER OF PATENTS AND TRADEMARKS
Washington, D.C. 20231

MF

cn

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR		ATTORNEY DOCKET NO.
08/994,878	12/19/97	EPSTEIN	M	PHA-23.313

LMC1/0911

JACK E HAKEN
US PHILIPS CORP
INTELLECTUAL PROP DEPT
580 WHITE PLAINS ROAD
TARRYTOWN NY 10591

EXAMINER	
SONG, H	
ART UNIT	PAPER NUMBER
2766	9

DATE MAILED: 09/11/00

Please find below and/or attached an Office communication concerning this application or proceeding.

Commissioner of Patents and Trademarks

Office Action Summary	Application No. 08/994,878	Applicant(s) Epstein	
	Examiner Ho S. Song		Group Art Unit 2766

☒ Responsive to communication(s) filed on *Jun 19, 2000* .

□ This action is **FINAL.**

□ Since this application is in condition for allowance except for formal matters, **prosecution as to the merits is closed** in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11; 453 O.G. 213.

A shortened statutory period for response to this action is set to expire *3* month(s), or thirty days, whichever is longer, from the mailing date of this communication. Failure to respond within the period for response will cause the application to become abandoned. (35 U.S.C. § 133). Extensions of time may be obtained under the provisions of 37 CFR 1.136(a).

Disposition of Claims

☒ Claim(s) *1-20* is/are pending in the application.

Of the above, claim(s) ______ is/are withdrawn from consideration.

□ Claim(s) ______ is/are allowed.

☒ Claim(s) *1-20* is/are rejected.

□ Claim(s) ______ is/are objected to.

□ Claims ______ are subject to restriction or election requirement.

Application Papers

□ See the attached Notice of Draftsperson's Patent Drawing Review, PTO-948.

□ The drawing(s) filed on ______ is/are objected to by the Examiner.

□ The proposed drawing correction, filed on ______ is □ approved □ disapproved.

□ The specification is objected to by the Examiner.

□ The oath or declaration is objected to by the Examiner.

Priority under 35 U.S.C. § 119

□ Acknowledgement is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d).

□ All □ Some* □ None of the CERTIFIED copies of the priority documents have been

□ received.

□ received in Application No. (Series Code/Serial Number) ______ .

□ received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

*Certified copies not received: ______ .

□ Acknowledgement is made of a claim for domestic priority under 35 U.S.C. § 119(e).

Attachment(s)

☒ Notice of References Cited, PTO-892

□ Information Disclosure Statement(s), PTO-1449, Paper No(s). ______

□ Interview Summary, PTO-413

□ Notice of Draftsperson's Patent Drawing Review, PTO-948

□ Notice of Informal Patent Application, PTO-152

--- *SEE OFFICE ACTION ON THE FOLLOWING PAGES* ---

DETAILED ACTION

1.. Claims 1-20 are pending. The previous grounds of rejection based on the Aziz and Scheier are withdrawn in view of Applicant's arguments in the Amendment filed 6/19/00. However, newly discovered prior art has necessitated new grounds of rejection. The new grounds of rejection are presented below. The delay in citation of the newly discovered prior art is regretted.

OBJECTION

2. The abstract of the disclosure is objected to because it contains more than 25 lines and 250 words. Correction is required. See MPEP § 608.01(b).

Claim Rejections - 35 USC § 102

> (e) the invention was described in a patent granted on an application for patent by another filed in the United States before the invention thereof by the applicant for patent, or on an international application by another who has fulfilled the requirements of paragraphs (1), (2), and (4) of section 371(c) of this title before the invention thereof by the applicant for patent.

3. Claims 5,7-11,13-18 are rejected under 35 U.S.C. 102(e) as being unpatentable by Trostle(US 5,919,257).

In claim 5, Trostle teaches user transmitting ID over the network in (col.5, lines 50-51). Trostle discloses reading from a storage data corresponding to the user having the received ID, which data comprises the user's private key encrypted using a key determined from identifying information of the user and sending via network the encrypted private key, whereby the encrypted key can be received and decrypted at the location of the user's identifying information in (col.5, lines 51-57). Trostle discloses destroying any non-volatile record of the private key at the location of the user in (col.6, lines 4-6).

In claims, 7-10, Trostle discloses receiving a digital signature manifesting the user's approval of a document, which digital signature represents a computed hash of the approved document encrypted using the user's private key and verifying the received digital signature by decrypting the digital signature using the user's public key and comparing the result of this decrypting with an independently computed hash of the document in (fig.6, col.2, lines 44-60, col.6, lines 10-25).

In claims 11,13-16, Trostle discloses computer storage and a server in (fig.1). Trostle discloses storage including respective IDs and encrypted private keys for the respective users in which private keys have been encrypted using respective keys determined from respective user identifying information and server reading an encrypted private key from the storage with corresponding to a particular user and transmitting the encrypted private key to the particular user in (fig.5 and col.5, lines 49-57).

In claims 17-18, see claims rejection 7-10 above.

Claim Rejections - 35 USC § 103

4. The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

5. Claims 1,3,4 are rejected under 35 U.S.C. 103(a) as being unpatentable over Trostle.

In claim 1, Trostle discloses user transmitting ID over the network in (col.5, lines 50-51). Trostle discloses reading from a storage data corresponding to the user having the received ID, which data comprises the user's private key encrypted using a key determined from identifying information of the user and sending via network the encrypted private key, whereby the encrypted key can be received and decrypted at the location of the user's identifying information in (col.5, lines 51-57). However, Trostle does not specifically discloses public key corresponding to the private key. The examiner asserts that Trostle teaches a scheme where by user transmitting username over the network and remote server compares username against a list and transmits corresponding private key to the user. It would have been obvious to person of ordinary skill in the art to include public key in a Trostle's system since private key is stored and transmitted over the network to the user. One of ordinary skill in the art would be motivated to use private/public key system in order to enhance data security and processing rate is much faster than symmetric key system.

In claims 3-4, Trostle discloses receiving a digital signature manifesting the user's approval of a document, which digital signature represents a computed hash of the approved document encrypted using the user's private key and verifying the received digital signature by decrypting the digital signature using the user's public key and comparing the result of this decrypting with an independently computed hash of the document in (fig.6, col.2, lines 44-60, col.6, lines 10-25).

6 Claims 2,6,12,19-20 are rejected under 35 U.S.C. 103(a) as being unpatentable over Trostle in view of Schneier.

In claims 2,6,12,19, Trostle discloses all the limitations above. However, Trostle does not discloses passphrase. Schneier discloses passphrase scheme in (page 174, passphrase section). It would have been obvious to one of ordinary skill in the art at the time the invention was made to use passphrase taught in Schneier for password of Trostle so that user can remember phrases easier than random character sequences. Passphrase provides greater security through increased entropy than a short password.

In claim 20, Trostle discloses at least one user terminal interconnected via network to the server(fig.1), in that user terminal is configured for transmitting to the server via the network an ID entered by the user, and receiving and decrypting an encrypted private key received via the network from the server using a user identifying information in (col.5, 50-57). Passphrase is discussed in claim rejction 2 above.

Conclusion

7 The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

a) Perlman (US 5,892,828) discloses a user log into the workstation with the user's password and workstation derives a secret encryption key by applying a known hash algorithm to the password prior to deleting it. The remote server returns the encrypted private key to the work station, which uses the secret key to decrypt and obtain the private key.

8. Any inquiry concerning this communication should be directed to Ho S. Song at telephone number (703)305-0042. The examiner can normally be reached on Monday through Friday from 7:30 am to 5:00 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gail Hayes, can be reached at (703)305-9711.

Any inquiry of a general nature or relating to the status of this application or preceeding should be directed to the group receptionist, whose telephone number is (703)305-3800.

Ho Song

Gail Hayes

GAIL O. HAYES
SUPERVISORY PATENT EXAMINER
GROUP 2700